VÄSTERÅS STAD

TJÄNSTEUTLÅTANDE

Datum
2023-01-04

Diarienr
NF 2022/00575- 2.2.3

Vård- och omsorgsförvaltningen
Anne Almqvist
Epost: anne.almqvist@vasteras.se

Kopia till
Kommunstyrelsen, Västerås stad

Nämnden för personer med funktionsnedsättning

Tjänsteutlåtande - Granskning av dataskyddsarbetet Nämnden för personer med funktionsnedsättning 2021

Förslag till beslut

Nämnden för personer med funktionsnedsättning tar del av rapporten daterad den14 mars 2022 och lägger den till handlingarna.

Ärendebeskrivning

Dataskyddsombuden ska enligt GDPR övervaka efterlevnaden av dataskyddslagstiftningen samt den personuppgiftsansvariges strategi för dataskyddsarbetet.

Detta är den första uppföljningsrapport som dataskyddsombuden gör i staden.

Bedömningen redovisas genom en modell där flera olika aspekter vägs ihop, för att spegla i vilken utsträckning den personuppgiftsansvariga organisationen arbetar ändamålsenligt med sitt dataskydd.

Dataskyddsombudens bedömning är att nämnden för personer med funktionsnedsättning har översikt och kontroll över sina personuppgiftsbehandlingar och arbetar strukturerat med dataskydd.

Vård- och omsorgsförvaltningen har till nämnden för personer med funktionsnedsättning lämnat följande förslag till beslut:

Nämnden för personer med funktionsnedsättning tar del av rapporten daterad den 14 mars 2022 och lägger den till handlingarna.

Från: kommunstyrelsen@vasteras.se
Skickat: den 16 november 2022 10:42
Till: Nämnden för personer med Funktionsnedsättning
Ämne: Granskning av dataskyddsarbetet 2021 - Nämnden för personer med funktionsnedsättning
Bifogade filer: Rapport NF granskning 2021.pdf

Uppföljningsflagga: Följ upp
Flagga: Har meddelandeflagga

Hej,

På grund av att en av våra anställda haft rollen som ensamt dataskyddsombud för hela staden under en period har återkoppling på nämndernas granskningsrapporter sammanställts senare än vad som först var tanken.

Granskningsrapporter är en del av stadens dataskyddsarbete och upprättas av stadens dataskyddsombud. Granskningsrapporten ska diarieföras och återrapporteras till nämnden, detta för att nämnden ska veta hur dataskyddsarbetet fungerar på just er nämnd.

Har nämnden frågor gällande granskningsrapporten för 2021 går det bra att ställa frågor till dataskyddsombud@vasteras.se.

Med vänlig hälsning,

Dataskyddsombuden

Västerås stad

Stadsledningskontoret

721 87 VÄSTERÅS

Telefon växel: 021-39 00 00

Dataskyddsombud@vasteras.se

http://www.vasteras.se

2022-03-14
Dnr: NF/

Dataskyddsombudens uppföljningsrapport 2021 för nämnden för personer med funktionsnedsättning

Stadsledningskontoret
721 87 Västerås
021-39 00 00 • www.vasteras.se

Robert Marcinkiewicz, dataskyddsombud
dataskyddsombud@vasteras.se

VÄSTERÅS STAD

Innehållsförteckning

1. Förkortningar

Dataskyddslagstiftning	GDPR samt nationell tilläggslagstiftning, ex. dataskyddslagen
DSO	Dataskyddsombud
EKMR	Europeiska konventionen för mänskliga rättigheter
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
GDPR	General Data Protection Regulation, även kallad dataskyddsförordningen på svenska
PUA	Personuppgiftsansvarig. I en kommun normalt styrelse och respektive nämnd
NF	Nämnden för personer med funktionsnedsättning

2. Bakgrund och rättsliga förutsättningar

Dataskyddsombuden ska enligt GDPR övervaka efterlevnaden av dataskyddslagstiftningen samt den personuppgiftsansvariges strategi för dataskyddsarbetet. Detta kan göras på olika sätt och det finns ännu inga bindande vägledningar, praxis eller liknande avseende metoden för detta.

Enligt GDPR ska dataskyddsombuden ges möjlighet att utan påverkan av personuppgiftsansvarig utforma och genomföra övervakningen och därefter ges möjlighet att rapportera sina slutsatser och rekommendationer till kommunstyrelse och nämnder. Dataskyddsombuden ska också ges möjlighet att utan påverkan få framföra sina slutsatser och rekommendationer, och ska heller inte motta någon form av direkta eller indirekta repressalier med anledning av dessa.

Dataskyddsombudets uppgift fråntar inte PUA:s ansvar att följa dataskyddslagstiftning, och att även kunna visa det (kallas även ansvarsskyldighet och är en av de sju grundläggande principerna i GDPR), utan ska ses som ytterligare ett verktyg för ökat skydd för den registrerade, och en hjälp till den personuppgiftsansvarige.

Detta är den första uppföljningsrapport som dataskyddsombuden gör i staden. För oss har det varit viktigt att det operativa arbetet har etablerats och att goda relationer mellan oss och förvaltningarna ska ha byggts upp, innan vi börjar följa upp. Detta för att uppföljningen ska kunna tas emot på ett förtroendefullt sätt och bli ett verktyg till fortsatt utveckling.

Vi vill också betona att uppföljningsarbetet är en lärande och prövande process i sig själv, och därför är vår intention att den ska förfinas och utvecklas, och därmed förändras, varje år.

3. Syfte och målbild

3.1. Allmänt

Tillvägagångsättet är framtaget efter inspiration av COSO-modellen[1], PMM-modellen[2], och GAPP-modellen[3] (alla tre internationellt erkända och etablerade modeller för intern kontroll och uppföljning av dataskyddsarbete) samt ett antal granskningsrapporter för andra kommuner.

Däremot ser vi att för att DSO:s uppföljning ska bli värdeskapande och leda till utveckling, behöver uppföljningen utgå mer från ett helhetsperspektiv än vad de etablerade modellerna gör. Endast kontroll av regelefterlevnad ger ett ensidigt fokus på ett område där det generellt sett är svårt att ge ett absolut svar om vad det innebär att följa regelverket eller inte. I de etablerade granskningsmodellerna ser vi också en övervikt av kontroll avseende olika typer av administrativa processer.

Vi menar att stället behöver dataskyddsarbetet ses som en ständigt pågående utvecklingsprocess där det största fokuset bör ligga på det långsiktiga strategiska perspektivet och riskhantering. Det innebär inte att de mer administrativa delarna är oviktiga, snarare är de många gånger grunden för att exempelvis risker ska upptäckas och kunna hanteras, men de får inte väga över och skymma helheten.

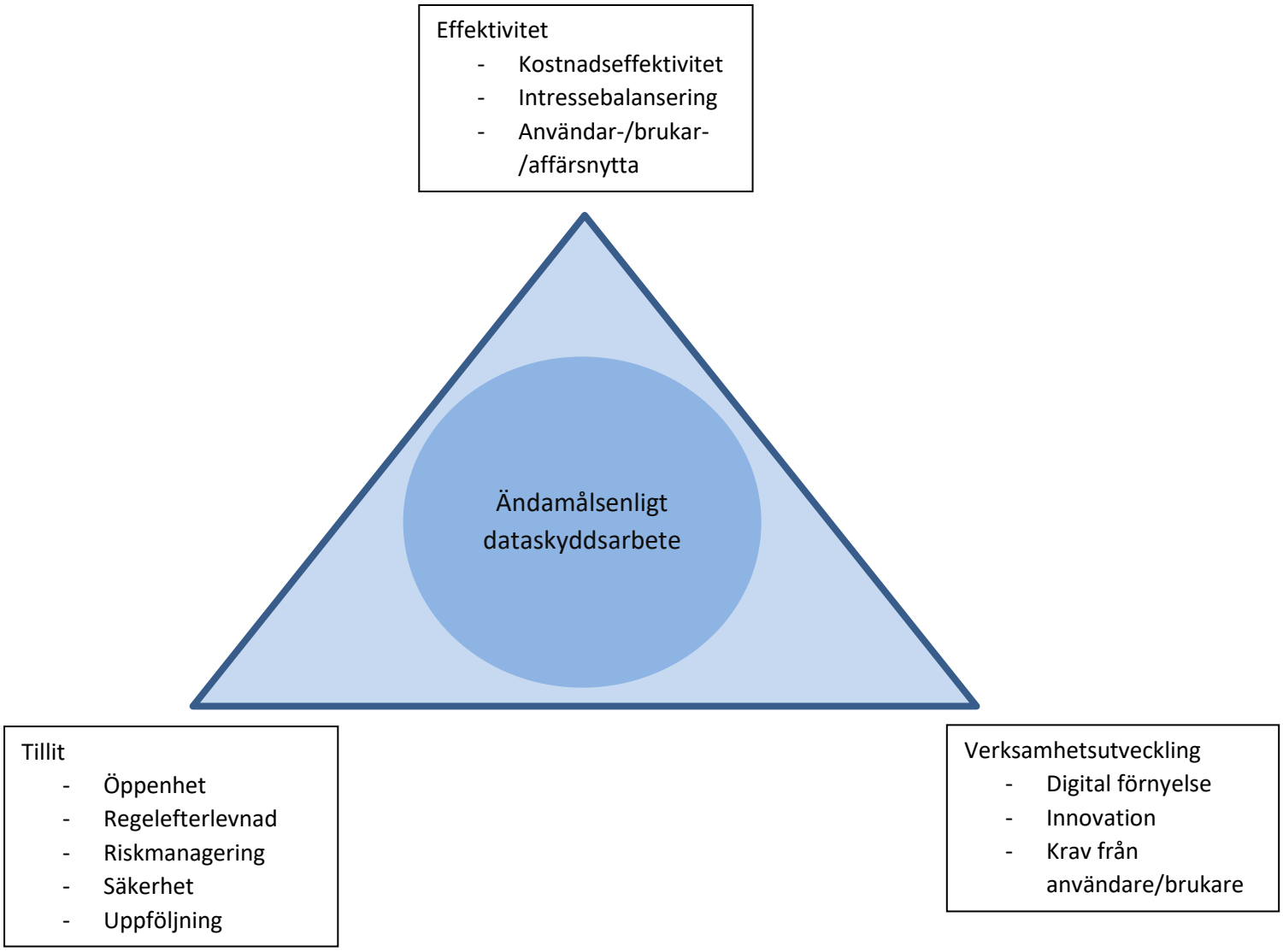
Vi ser att eftersom våra normer och värderingar, behov och tekniska möjligheter hela tiden utvecklas, ändras hela tiden förutsättningarna för dataskydd, och bedömningar behöver konsekvent ändras. Därför är det viktigare för en organisation att skapa förmåga att agera utifrån de föränderliga

[1] Intern kontroll | PwC, 2022-03-14
[2] Measuring a privacy program (cpacanada.ca), 2022-03-14
[3] Generally Accepted Privacy Principles - Wikipedia, 2022-03-14

omständigheterna, än att ha prickfria administrativa rutiner. Och den här förmågan bygger i stor utsträckning på organisationskulturen, kompetens, arbetssätt med mera.

Dataskyddsombuden i Västerås arbetar med den lagstadgade ”övervakningen” på olika sätt, men främst genom att vara involverad i verksamheten och där ge råd och stöd. Vi gör också en särskild granskning av några utvalda områden, där varje PUA får svara på ett antal frågor kopplade till de utvalda områdena.

Vår bedömning redovisas genom en modell där flera olika aspekter vägs ihop, för att spegla i vilken utsträckning den personuppgiftsansvariga organisationen arbetar ändamålsenligt med sitt dataskydd.



3.2. Ändamålsenligt dataskyddsarbete

Att arbeta med dataskydd och uppfylla dataskyddslagstiftningens krav är ett mångfacetterat och komplext arbete. Det är en vanlig beskrivning att det handlar mer om ett förändringsarbete än juridik, eftersom det består av så många olika komponenter. I grunden syftar alla regler till att skydda människors grundläggande rättighet till skydd för sitt privatliv.[4] Men rätten till det skyddet tar

[4] EKMR, art. 8, EU-stadgan art. 3, 7, 8

inte ut andra rättigheter,[5] exempelvis rätten till utbildning,[6] rätten till fysisk säkerhet[7] eller rätten till god förvaltning.[8]

Lagstiftningen är komplex eftersom den innehåller allt från detaljerade administrativa krav om exempelvis vad ett registerutdrag ska innehålla, till mer allmänna krav såsom uppgiftsminimeringsprincipen, till mycket överskådliga målbilder såsom att dataskyddet i så stor utsträckning som möjligt ska vara inbyggt (”privacy by design”). Dessutom är GDPR i stor utsträckning uppbyggd på ”normer”, där det är meningen att innebörden, och därmed tillämpningen av lagstiftningen, ska kunna förändras. Exempelvis finns krav på att säkerhetsnivån ska vara enligt ”best practise”, men vad det de facto innebär är naturligtvis föränderligt.

I dagsläget, och för många år framåt, är dessutom de allra flesta personuppgiftsansvariga organisationer i en fas där man fortfarande ställer om till de nya krav och normer som GDPR och senaste praxis innebär.

Sammantaget innebär detta att triangeln hela tiden måste vara balanserad eftersom behov och krav ständigt förändras, tillsammans med teknisk utveckling. Samtidigt är dataskyddsperspektivet en del av alla olika hörn i triangeln; ex. innebär ett kostnadseffektivt arbetssätt att göra rätt från början, och det i sin tur, kan exempelvis innebära att dataskyddsperspektivet beaktas tidigt i en utvecklingsprocess. På så sätt kan man undvika att utveckla ex. ett arbetssätt som senare visar sig vara otillåtet, eller undvika att köpa in ett system där det senare visar sig att det innebär stora legala risker.

3.3. Effektivitet

Områden vi utvärderar särskilt i denna uppföljning, avseende hur effektivt kommunstyrelsens dataskyddsarbete är följande;

- Operativ organisation inklusive styrning
- Samspelet mellan förvaltningen och dataskyddsombud
- Interna arbetssätt och hur dessa efterlevs
- Långsiktigheten i de åtgärder som genomförs
- Intresse och engagemang från förtroendevalda i kommunstyrelsen och förvaltningens ledning

[5] Se resonemang i GDPR, skäl 4
[6] EKMR tilläggsprotokoll, art. 2
[7] EKMR, art. 5, EU-stadgan art. 6
[8] EU-stadgan, art. 41

- I vilken grad DSO involveras tidigt i olika typer av processer (för att tidigt eliminera hinder och lösa problem)

3.4. Verksamhetsutveckling

Eftersom nästan alla verksamheter inkluderar någon form av personuppgiftsbehandling innebär utveckling av dessa verksamheter att man även behöver inkludera dataskyddsperspektivet. På samma sätt som man exempelvis belyser de ekonomiska aspekterna i olika typer av utvecklingsfrågor. När det gäller verksamhetsutveckling genom digitalisering är dataskyddsperspektivet ännu viktigare.

Områden vi utvärderar särskilt i denna uppföljning, avseende hur dataskyddsperspektivet integreras i verksamhetsutvecklingsarbetet är följande;

- Hur personuppgiftsincidenter utnyttjas för att skapa lärande och utveckling,
- Hur dataskyddsombuden och/eller annan dataskyddsexpertis involveras i olika typer av utvecklingsarbeten,
- Hur beaktas dataskyddsperspektivet i det tekniska utvecklingsarbetet

3.5. Tillit

Att uppnå total regelefterlevnad avseende dataskydd, i en kommun är sannolikt varken möjligt eller eftersträvansvärt. Dels för att det i de allra flesta fall inte går att definitivt avgöra när lagregler efterlevs och när så inte är fallet. Dels för att verksamheten är så komplex och mångfacetterad, samtidigt som mängden behandlingar är så stora, att insatserna för att nå total regelefterlevnad är oöverblickbara. Men eftersom olika typer av personuppgiftbehandlingar ofta är oundgängliga för den digitala utvecklingen, är exempelvis en kommun beroende av att både invånare och medarbetare vill lämna sina personuppgifter till kommunen, annars blir digitaliseringen omöjlig. Det innebär i sin tur att invånare och medarbetare behöver känna tillit till kommunens hantering.

Områden vi utvärderar särskilt i denna uppföljning, avseende hur NF arbetar med att invånare och medarbetare ska känna tillit till NF:s hantering av deras personuppgifter är följande;

- Hur NF arbetar med att skaffa sig kontroll och översikt över de personuppgiftsbehandlingar man ansvarar för,
- Hur NF utifrån ett systematiskt perspektiv arbetar för att efterleva dataskyddslagstiftning,
- Hur NF arbetar med att efterleva GDPR:s krav om öppenhet gentemot den registrerade

- Hur NF arbetar med att kommunicera kring integritet med medarbetare och invånare

4. Särskilda granskningsfrågor 2021

4.1. Incidenter

DSO har avseende NF inte följt upp någon incident, dock har respektive PUA besvarat hur man informerar sin personal avseende phishingmail. Det vill säga vilka åtgärder PUA har vidtagit för att minska risken att personal inte klickar på misstänkta länkar i mail/SMS. DSO har specifikt lyft denna fråga eftersom den innebär en hög risk för samtliga PUA, phishingmail-attacker är även något som ökat markant senaste tiden.

NF har redogjort att man inte vidtagit vidare åtgärder utan hänvisat sina medarbetare till den stadsövergripande informationen gällande phishingmail. DSO kan vidare konstatera att incidenterna som rapporterats inom VOF 2021 som DSO inte har valt att följa upp har hanterats på ett effektivt sätt. DSO har inget övrigt att anmärka på avseende hur NF har hanterat incidenter.

4.2. Etablering av dataskyddsorganisation

DSO:s bedömning är att NF redan när GDPR trädde i kraft tagit frågan på allvar och arbetat strukturerat. Ett antal medarbetare på förvaltningen har från början arbetat med dataskydd och man har på det sättet byggt upp en gedigen intern kompetens. DSO ser även den positiva effekten av att ha en utpekad person som leder arbetet med dataskyddsfrågor på förvaltningen. Vidare har förvaltningen involverat DSO i strategiska frågor och planer framåt vilket påvisar att man förstått att det är viktigt med dataskyddsfrågor. Högsta ledningen för förvaltningen och den politiska ledningen i de olika nämnderna har även visat engagemang och ställt egna frågor.

I denna granskning har DSO ställt frågor om olika typer av kontaktfunktioner för DSO samt namn på personer med operativt ansvar i olika delar av dataskyddsarbetet. Vård- och omsorgsförvaltningen har som nämnt ovan en dataskyddsgrupp där uppdraget har konkretiserats och beslutats. Vård- och omsorgsförvaltningen anger vidare i sitt svar att man har månatliga möten där aktiviteter och potentiella brister tas upp i respektive förvaltningsplan för objekten. Arbetet pågår fortlöpande och vidare planeras ett årshjul som ska påvisa kommande aktiviteter.

Det finns vidare ett tydligt ägandeskap på förvaltningsnivå med arbetet av dataskydd vilket DSO tror är en stor framgångsfaktor. Detta innebär att dataskyddsfrågor tas på stort allvar och anses vara en lika viktig del som exempelvis ekonomi eller digitalisering.

4.3. Registerförteckning

Registerförteckningen, förutom att det är ett lagkrav så är det en grundläggande del av dataskyddsarbetet eftersom det innebär att respektive personuppgiftsansvarig har en översikt och kontroll över de personuppgiftsbehandlingarna som man ansvarar för. Saknar den personuppgiftsansvarige en registerförteckning saknar man kontroll över sina personuppgiftsbehandlingar vilket innebär en hög risk.

DSO har mottagit nämndens registerförteckning och bedömer att den håller en god kvalitet samt att man efterlever lagkraven.

DSO har vidare efterfrågat en beskrivning hur NF harbetar med att hålla sin registerförteckning aktuellt och uppdaterad. NF svarar att registerförteckningen årligen granskas och att man har rutiner så att nya behandlingar förs in i registerförteckningen vid exempelvis inköp av nytt IT-verktyg.

Sammantaget bedömer DSO att NF har ett sammanhållet och systematiserat arbetssätt avseende registerförteckningen.

5. Risker utifrån 2021 års granskning

5.1. Effektivitet, verksamhetsutveckling och tillit

DSO bedömning är att NF har översikt och kontroll över sina personuppgiftsbehandlingar och arbetar strukturerat med dataskydd.

6. Styrkor utifrån 2021 års granskning

6.1. Effektivitet, Verksamhetsutveckling

DSO vill lyfta samarbetet mellan DSO och Vård- och omsorgsförvaltningens dataskyddsgrupp som ett bra exempel. Vård- och omsorgsförvaltningen har förstått att dataskydd är en viktig strategiskt fråga eftersom de involverat DSO i strategiska diskussioner och planer framåt.

DSO upplever att dataskyddsgruppen tar ett eget stort operativt ansvar eftersom man byggt upp en gedigen intern kompetens. Det leder även till att arbetet blir mer tidseffektivt.

6.2. Tillit

Dataskyddsombudens bedömning är att NF i dagsläget har kontroll över sina personuppgiftsbehandlingar. Kontroll innebär att man kan arbeta riskbaserat, har en beredskap för incidenter och kan prioritera akuta risker. Vidare innebär det även att man på ett effektivt sätt kan besvara frågor från invånare och anställda avseende sina personuppgiftsbehandlingar. Eftersom man har kontroll innebär det även att registerutdrag kan hanteras på ett effektivt sätt. Vård- och omsorgsförvaltningen har en fungerande dataskyddsorganisation där man byggt upp en gedigen kompetens och har tagit stort operativt ansvar när det gäller dataskyddsfrågor.

7. Dataskyddsombudens råd

7.1. Ledningens kunskap och engagemang

Olika typer av integritets- och säkerhetsfrågor, kopplat till hantering av personuppgifter, är på lång sikt en av de strategiskt viktigaste frågorna för kommuner. DSO bedömning är både den högsta ledningen och de olika politiska nämnderna inom Vård- och omsorgsförvaltningen har visat engagemang för dataskyddsfrågor. DSO har inga råd att ge utan hoppas att Vård- och omsorgsförvaltningen fortsätter att lyfta dataskyddsperspektivet i olika strategiska vägvalsfrågor.

7.2. Ägandeskap av nämnden för personer med funktionsnedsättnings dataskyddsarbete och det operativa dataskyddsarbetet

Inom Vård- och omsorgsförvaltningen har det byggts upp en gedigen kompetens. DSO hoppas att det fortsatt finns ett tydligt ägandeskap och att resurser läggs på det operativa dataskyddsarbetet.